

2017196

by Jack Rogers

Submission date: 30-Apr-2024 09:37PM (UTC+0100)

Submission ID: 231572657

File name: 16489_Jack_Rogers_2017196_183168_1456779762.pdf (346.61K)

Word count: 3219

Character count: 22071

Your Name: Jack Rogers

University Number: 2017196

Course: BSc Electrical / Electronic Engineering

Module Code: SGEE6005

Assignment Title: Internet of Things

Date Submitted: 30/04/2024

Word Count: 2864 words

Table of Contents

1. Executive Summary	4
2. Introduction.....	5
3. Key Concepts of IoT and Industry 4.0 (Nawi System)	6
3.1 Internet of Things (IoT) Definitions	6
3.2 Enabling Technologies.....	6
3.2.1 Sensors.....	6
3.2.2 Actuators	7
3.2.3 Communication Protocols	7
3.2.4 Data Analytics	8
3.3 Connectivity Models	8
3.3.1 Device to Device (D2D)	8
3.3.2 Device to Cloud (D2C).....	8
3.3.3 Device to Gateway (D2G)	9
3.3.4 Back-end Data Sharing	9
3.4 Transformational Potential	9
3.4.1 Enhanced Efficiency	9
3.4.2 Improved Decision-Making	9
3.4.3 Cost Savings	9
3.4.4 New Business Opportunities.....	9
4. Security and Privacy Challenges (Nawi System)	10
4.1 Security Concerns	10
4.1.1 Vulnerabilities	10
4.1.2 Data Breaches.....	10
4.1.3 Cyber-attacks.....	10
4.2 Privacy Issues	10
4.2.1 Consent	10
4.2.2 Data Ownership	11
4.2.3 Surveillance	11
4.3 Regulatory Framework	11
4.3.1 NIST Cybersecurity Framework	11
4.3.2 General Data Protection Regulation (GDPR).....	11
4.3.3 Industry-specific Standards	11
5. Analysis and Evaluation	12
6. Conclusion	13
7. References	14

Figure 1 - Scada System Structure 5

Figure 2 - PT100 Sensor 6

Figure 3 - Siemens Drives 7

Figure 4 - ProfiNet 8

1. Executive Summary

Firstly, an explanation on IoT and its application in SCADA was made while highlighting the connectivity and data-driven nature of IoT within the company. Key enabling technologies such as sensors, actuators, communication protocols, and data analytics were researched, and highlighting their roles in real-time monitoring and control.

A number of connectivity models were discussed, including device-to-device, device-to-cloud, and device-to-gateway. Back-end data sharing between SCADA systems and the company applications was highlighted.

The potential of IoT integration within the Nawi SCADA system was explained, with a focus on improved efficiency, improved decision-making, cost savings, and new business opportunities. Security and privacy challenges were also looked at, including vulnerabilities, data breaches, and privacy issues, needing strong cybersecurity measures and compliance with regulatory frameworks.

Finally, the research highlighted the importance of addressing security and privacy concerns for responsible deployment of IoT-enabled SCADA systems. By including regulatory frameworks such as the NIST Cybersecurity Framework and GDPR alongside technical safeguards, that the company can maximise the benefits of IoT integration while minimising risks.

2. Introduction

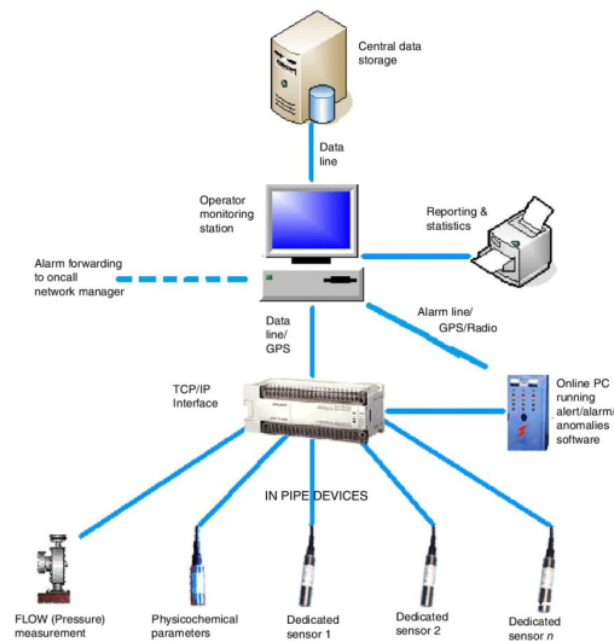


Figure 1 - Scada System Structure

The development of the Internet of Things (IoT) and Industry 4.0 has brought about a large number of advances in digital technology and the development of various industries. One example of key applications of these technologies is supervisory control and data acquisition (SCADA) systems, which play a key role in monitoring and controlling industrial processes. The integration of SCADA systems into IoT and Industry 4.0 ecosystems can present a number of challenges, especially when it comes to security and privacy. This research assignment critically analyses the key concepts of the Internet of Things and Industry 4.0 in the context of a SCADA system that applies to the workplace known as the Nawi System, followed by research on the security and privacy issues that may arise. Figure 1 shows the basic structure and design of a SCADA system and what is needed to implement it. (GmbH, 2024)

3. Key Concepts of IoT and Industry 4.0 (Nawi System)

3.1 Internet of Things (IoT) Definitions

The Internet of Things (IoT) refers to a network of interconnected devices embedded with sensors, software, and other technologies that enable them to collect and exchange data. In the context of Supervisory Control and Data Acquisition (SCADA) systems, IoT integration involves connecting industrial sensors, actuators, and controllers to a network setup, allowing for remote monitoring and control of industrial processes. (Oracle, 2024)

The definition of IoT varies across industries. Some definitions focus on the connectivity aspect, highlighting the continuous communication between devices and backend systems. Others point out the data-driven nature of IoT, highlighting the importance of data analytics and insights derived from sensor data. In the context of the Nawi SCADA system, IoT represents the merging of operational technology (OT) with information technology (IT), allowing the digitisation and automation of industrial processes while receiving and giving the appropriate data needed for its application. (Meredith, 2024)

3.2 Enabling Technologies

3.2.1 Sensors

Sensors play a crucial role in IoT-enabled SCADA systems by collecting data from various sources, including temperature, pressure, flow rates, and other process variables. These sensors can be wired or wireless and are essential for monitoring and controlling industrial processes in real-time. In the context of the Nawi system the sensors are used to measure the temperature of the storage area and feedback in real time what it is. This temperature can also be monitored and controlled as it is an IoT enabled system. One example of a temperature sensor that is used in this system is a PT100 RTD. (David, 2024) (Ltd, 2024)

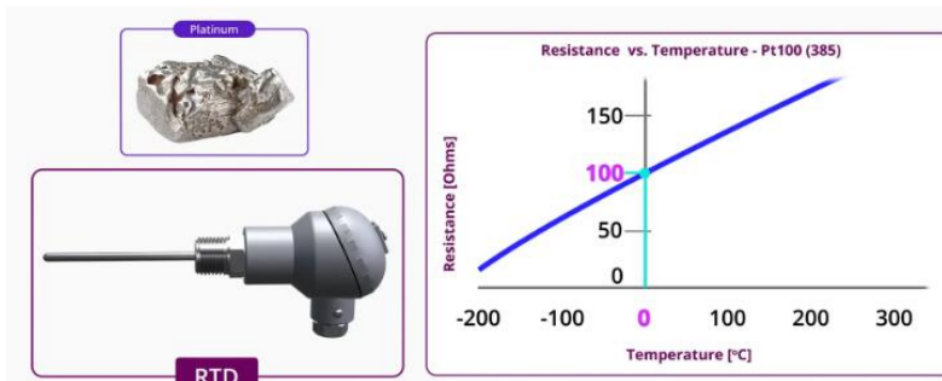


Figure 2 - PT100 Sensor

3.2.2 Actuators

Actuators are devices that convert electrical signals into physical action, allowing SCADA systems to control industrial equipment remotely. Examples include motors, valves, and relays, which can be activated or deactivated based on commands received from the SCADA system. In the context of the Nawi system the actuators in this case would be the cranes as they can be remotely driven, and its state is also monitored by electrical signals showing what the crane is doing in real time.



Figure 3 - Siemens Drives

For example, if the crane was in the incorrect position, then the IoT enabled system would allow the user to control its movements remotely without having to go to the crane itself. It is also used for dictating how many locations are full and empty all on one screen therefore an order can be made for the crane to gather what it needs remotely on the system. (N, 2024)

3.2.3 Communication Protocols

Communication protocols define the rules and standards for data exchange between IoT devices and backend systems. In SCADA systems, common communication protocols include ModBus, MQTT, DDS and ProfiNet. These protocols ensure reliable and secure transmission of data between sensors, controllers, and the SCADA server.



Figure 4 - ProfiNet

In the context of the Nawi system ProfiNet TCP is used as a communication protocol for the Siemens PLC 1500 in the system as it can then open up an option to use TIA portal and control its actuators remotely on one server by using the same IP address, and process data with addresses. (IoT, 2024)

3.2.4 Data Analytics

Data analytics tools and techniques are essential for extracting actionable insights from the vast amounts of data generated by IoT-enabled SCADA systems. By analysing historical data trends, predicting future outcomes, and identifying anomalies, data analytics empower organizations to optimize industrial processes, improve efficiency, and reduce downtime. In this case the data analytics are used to monitor the rate of change in the temperature of the storage are as well as data for the efficiency of the cranes. (High Tide Technologies, 2024)

3.3 Connectivity Models

3.3.1 Device to Device (D2D)

In D2D connectivity model, IoT devices communicate directly with each other without the need for intermediate gateways or cloud services. This model is suitable for peer-to-peer communication between sensors and actuators within a localized network environment. In this case for the Nawi Scada system as ProfiNet is being used these devices can communicate with each other directly as they are all controlled of the same network. (AgileVision.io, 2024)

3.3.2 Device to Cloud (D2C)

In the D2C connectivity model, IoT devices send data to cloud servers for storage, analysis and processing. This model enables centralized data management, remote access and scalability, making it ideal for large-scale multi-site SCADA deployments. (Kraeling, 2024)

3.3.3 Device to Gateway (D2G)

In the D2G connectivity model, IoT devices communicate with a gateway device that acts as an in-between for the devices and the backend systems. The gateway collects data from multiple devices and performs local processing and forwards relevant information to a SCADA server or cloud platform. (Zain, 2024)

3.3.4 Back-end Data Sharing

Back-end data sharing involves sharing data between SCADA systems and enterprise applications such as ERP (Enterprise Resource Planning) systems, MES (Manufacturing Execution Systems), and CRM (Customer Relationship Management) systems. This integration enables seamless data exchange, synchronization, and collaboration between operational and business systems, driving efficiency and productivity gains.

3.4 Transformational Potential

3.4.1 Enhanced Efficiency

By enabling real-time monitoring, predictive maintenance, and optimization of industrial processes, IoT-enabled SCADA systems can improve efficiency, reduce downtime, and minimize resource wastage. In this case the Nawi system helps minimize waste product as it monitors the locations for the storage area, where in some none IoT integrated systems a manual check of the locations would be done to recover the waste product, the Nawi system can automatically check which product is near its due date and would prioritize that over other. In the context of the Nawi system, it also helps minimize downtime as instead of having to go into the are to control the cranes, this can be remotely done anywhere as long as the same server is in use. (Advanced Technology Services, 2024)

3.4.2 Improved Decision-Making

The availability of real-time data and actionable insights enables informed decision-making at all levels of the company, from frontline operators to senior management. This data-driven approach facilitates proactive management of assets, resources, and operations, leading to better outcomes and competitive advantages.

3.4.3 Cost Savings

The Nawi SCADA system can help reduce operational costs by improving energy consumption, reorganisation workflows, and automating repetitive tasks. Additionally, predictive maintenance capabilities minimise unplanned downtime and extend the lifespan of critical equipment, resulting in significant cost savings over time.

3.4.4 New Business Opportunities

IoT integration opens up new business opportunities and income flows by enabling new products and services. As the Nawi system uses IoT data to offer value-added services such as remote monitoring, asset tracking, and performance optimization, creating new sources of revenue and enhancing customer satisfaction.

However, along with its potential, IoT integration in SCADA systems also presents challenges such as cybersecurity risks, data privacy concerns, interoperability issues, and regulatory compliance requirements. Addressing these challenges requires a holistic approach that encompasses technical, organizational, and regulatory measures to ensure the secure and responsible deployment of IoT-enabled SCADA systems.

4. Security and Privacy Challenges (Nawi System)

4.1 Security Concerns

4.1.1 Vulnerabilities

The Nawi SCADA system can be vulnerable to a wide range of security vulnerabilities, including weak authentication mechanisms, outdated software, insecure communication protocols, and lack of encryption. These vulnerabilities can be exploited by malicious competitors to gain unauthorised access to the SCADA network, manipulate industrial processes, or disrupt critical infrastructure. For example, if the system was used by the Siemens web server then with very little information of IP addresses and component addresses then they could log in and control the company's system. There are many ways to avoid this type of vulnerability but in this case a custom server was made and an authorisation code is needed to gain access to the company's network, and a wall of protection is there.

4.1.2 Data Breaches

Data breaches can pose a significant threat to the Nawi SCADA system, as they can result in unauthorised access to sensitive information, such as operational data, production schedules, and equipment configurations. A breach in the Nawi SCADA system can have influential consequences, including financial losses, reputational damage, and safety risks. To minimise this an authorisation code is needed along with certain access to company Management and supervisors is put in place.

4.1.3 Cyber-attacks

The Nawi SCADA systems can be a target for cyber-attacks due to its critical role in company operations. Common cyber-attacks targeting SCADA systems include malware infections, ransomware attacks, denial-of-service (DoS) attacks, and insider threats. These attacks can disrupt industrial processes, cause equipment damage, and compromise safety systems, leading to severe consequences for organizations and society at large. (Ltd E. , 2024)

4.2 Privacy Issues

4.2.1 Consent

In the Nawi SCADA systems, data is collected from various sources, including sensors, controllers, and actuators. Without obtaining consent from Managers the company's database whose data is being collected raises ethical concerns regarding the use of personal data and the potential for privacy violations.

4.2.2 Data Ownership

Another privacy concern in SCADA systems is the ownership of data generated by IoT devices. In many cases, the ownership of this data is ambiguous, leading to disputes over who has the right to access, use, and share it. Clear guidelines and agreements are needed to establish ownership rights and responsibilities regarding SCADA data. In this case the company has full ownership of the Nawi SCADA system and its collected data within its work are to minimise outside competitors gaining access and breaching their data.

4.2.3 Surveillance

The wide spread deployment of IoT devices in SCADA systems has raised concerns about mass surveillance and data collection practices. Organisations may collect and analyse data from SCADA systems for purposes beyond their original intent, leading to privacy infringements and surveillance abuses. Transparency and accountability measures are essential to address these concerns and ensure that data collection practices are ethical and lawful.

4.3 Regulatory Framework

4.3.1 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidelines and best practices for managing cybersecurity risks in critical infrastructure, including in the Nawi SCADA system. The framework highlights risk management, continuous monitoring, and incident response to enhance the resilience of SCADA network against cyber threats.

4.3.2 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) imposes strict requirements on the company's collection, processing, and protection of personal data. The Nawi SCADA system that handles company data does comply with GDPR requirements, as it includes data minimisation, purpose limitation, and data subject rights, to ensure the privacy and security of company's information.

4.3.3 Industry-specific Standards

By using the Nawi SCADA System, the product needs to be tracked as soon as it enters the warehouse, throughout the production lines and gets dispatched to the customer in order to comply with the company's food safety standards. If the product was not tracked, then this could cause unhappy customers as the product could go missing and result in a loss.

5. Analysis and Evaluation

The provided research offers a detailed overview of IoT integration within SCADA systems with a focus on the Nawi system. It covers key concepts, essential technologies, connectivity models and transformative potentials, followed by a consideration of security and privacy issues along with relevant regulatory frameworks.

A strong part of this research is in the detailed explanation of IoT components and their roles in the Nawi SCADA system, such as temperature sensors for data collection and actuators for remote control. The uses of communication protocols such as ProfiNet TCP and the highlighting on data analysis underline the potential of the Nawi system in optimising industrial processes.

Also, the analysis of connectivity models clarifies how IoT devices in the Nawi system interact, through direct device-to-device communication. This provides a clear understanding of the system's design and its potential.

The research also shows several security and privacy issues that can occur in the Nawi SCADA system, especially for the Nawi system. Vulnerabilities such as weak authentication mechanisms and potential data breaches feature the need for robust cybersecurity measures. Incorporating regulatory frameworks such as the NIST Cybersecurity Framework and GDPR demonstrates awareness of legal and compliance aspects, increases system resilience against cyber threats, and ensures data privacy.

6. Conclusion

The research provides full research on IoT integration within the Nawi SCADA system. It explains key concepts, enabling technologies, connectivity models, and transformational potentials, offering valuable insights into the system's operation and benefits.

The research also shows significant security and privacy challenges inherent in IoT-enabled SCADA systems. Vulnerabilities, data breaches, and potential cyber-attacks pose serious threats to system reliability and operational stability, needing strong cybersecurity measures and controlling compliance.

By integrating regulatory frameworks like the NIST Cybersecurity Framework and GDPR, alongside technical safeguards, the research highlights a secure approach to IoT implementation. This approach ensures operational efficiency, data privacy, and regulatory compliance, while maximising the potential of IoT integration within the Nawi SCADA system.

In conclusion, the research points out the transformative impact of IoT on industrial processes while highlighting the obligation of addressing security and privacy concerns for sustainable and responsible use. It serves as a valuable resource for the company seeking to use the benefits of IoT within the Nawi SCADA systems while minimising risks.

7. References

- Advanced Technology Services, I. (2024, 12 4). *What is SCADA & how can it Improve Production Efficiency?* Retrieved from ATS: <https://www.advancedtech.com/blog/what-is-scada/>
- AgileVision.io. (2024, 4 24). *AgileVision.io*. Retrieved from Overview of IoT Device Communication: [https://www.agilevision.io/blog/overview-of-iot-device-communication/#:~:text=Device%2Dto%2DDevice%20\(D2D,central%20hub%20or%20network%20infrastructure.](https://www.agilevision.io/blog/overview-of-iot-device-communication/#:~:text=Device%2Dto%2DDevice%20(D2D,central%20hub%20or%20network%20infrastructure.)
- David. (2024, 3 17). *The potential of temperature sensor applications in IoT*. Retrieved from DeepSea Developments: [https://www.deepseadev.com/en/blog/temperature-sensor-applications/#:~:text=Thermistors%20are%20popular%20IoT%20temperature,\) %2C%20and%20infrared%20temperature%20sensors.](https://www.deepseadev.com/en/blog/temperature-sensor-applications/#:~:text=Thermistors%20are%20popular%20IoT%20temperature,) %2C%20and%20infrared%20temperature%20sensors.)
- GmbH, H. (2024, 04 18). *An explanation of SCADA in the age of IoT*. Retrieved from Heisenware: <https://heisenware.com/en/info/scada-iot/#:~:text=SCADA%20systems%20leverage%20the%20power,improved%20process%20controls%20and%20efficiencies.>
- High Tide Technologies, L. (2024, 03 27). *htt.io*. Retrieved from Integrating SCADA and Data Analytics: <https://htt.io/resources/integrating-scada-and-data-analytics/#:~:text=SCADA%20systems%20harness%20the%20power,context%20of%20water%20system%20dynamics.>
- IoT, T. (2024, 3 24). *What Are the IoT Communications and Protocols?* Retrieved from iot.telenor.com: <https://iot.telenor.com/iot-insights/what-is-iot-communications-protocols/>
- Kraeling, M. (2024, 4 6). *Internet of Things*. Retrieved from Science Direct: <https://www.sciencedirect.com/topics/engineering/device-to-device-communication/#:~:text=Internet%20of%20Things&text=In%20the%20device%2Dto%2Dcloud,data%20and%20control%20of%20communications.>
- Ltd, E. (2024, 04 20). *SCADA vulnerabilities and attacks*. Retrieved from Science Direct: <https://www.sciencedirect.com/science/article/pii/S0167404822004205>
- Ltd, P. S. (2024, 3 15). *What Is RTD Sensor And How Does It Work?* Retrieved from Peaksensors.com: <https://peaksensors.com/blog/resistance-thermometer/what-is-rtd-sensor-and-how-does-it-work/>
- Meredith, D. (2024, 25 2). *What Is the Internet of Things (IoT)? How It Works and Benefits*. Retrieved from Investopedia: <https://www.investopedia.com/terms/i/internet-things.asp>
- N, A. (2024, 3 20). *An Expert Guide to Actuators in IoT*. Retrieved from Nabto: <https://www.nabto.com/actuators-in-iot-guide/#:~:text=What%20Are%20Actuators%20in%20IoT,chosen%20settings%20of%20the%20user.>
- Oracle. (2024, 20 2). *What is IoT?* Retrieved from Oracle.com: <https://www.oracle.com/uk/internet-of-things/what-is-iot/#:~:text=What%20is%20IoT%3F,and%20systems%20over%20the%20internet.>

Zain, I. (2024, 4 10). *Internet of Things*. Retrieved from IJEDR:
<https://www.ijedr.org/papers/IJEDR1603172.pdf>

FINAL GRADE

GENERAL COMMENTS

70/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

RESEARCH-INFORMED LITERATURE



There was evidence of further reading and research with the inclusion of a reference list and appropriate in text referencing. Your interpretation and understanding of the additional research was good. Your references were appropriate to the task and your reference list was of an appropriate length for this assignment.

13

KNOWLEDGE AND UNDERSTANDING



The knowledge and understanding of the subject demonstrated by this assignment was reasonably extensive. There were very few gaps in your knowledge of the basic principles and your understanding of the higher level concepts was demonstrated to a limited degree. You have demonstrated some critical understanding of the main concepts and expanded your knowledge beyond that contained in the course notes, however your explanations need to be more detailed and written with a greater emphasis on critical evaluation rather than description.

20

ANALYSIS



Your analysis of the task was generally very good, both in class and as shown in this assignment. You have demonstrated sound critical analysis skills and your approach to the task was logical. You carried out a detailed evaluation of the results and included a good conclusion relating the practical results to researched theory. The conclusions demonstrated very good cognitive skills and the ability to interpret quantitative and qualitative data without error.

29

PRACTICAL APPLICATION AND DEP.

SKILLS FOR PROFESSIONAL PRAC.



Your written report was generally good and contained most of the required detail, it was also written in a coherent and logical way. The available word count was in the main effectively used.

8